BUNDESREPUBLIK DEUTSCHLAND

Bescheinigung

Die DeTeMobil Deutsche Telekom MobilNet GmbH in Bonn/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk"

am 17. März 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole H 04 L und H 04 Q der Internationalen Patentklassifikation erhalten.

München, den 22. April 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag
Faust

Aktenzeichen: 199 11 782.9

A 9161
06.90
11/98

Allgemeine Anweisungen General Instructions

I. Folgende Schriftstücke bitte ich, mir zu übersenden: Stück / Copies
You are requested to provide the following documents:

1. Ausländische Anmeldung wie eingereicht 2
Foreign application, as filed

2. Amtliche Empfangsbestätigung 2
Official certificate of receipt

3. Irgendwelche während der Weiterbehandlung der Anmeldung bei Ihrem Patentamt eingereichten Unterlagen 2
Any and all documents filed at your Patent Office in the course of application pursuance

4. Detaillierte Gebührenrechnung 2
Detailed bill of costs

II. Bitte halten Sie sich an folgende Anweisungen:
You are requested to comply with the following instructions:

1. Der Auftrag erfolgt im Namen und für Rechnung meines Mandanten.
You are briefed in the name and for account of my client.

2. Alle Patente und Anmeldungen sind durch Einzahlung der Gebühren, Steuern usw. aufrechtzuerhalten, falls Sie bis zum Fälligkeitsdatum von mir nicht anderweitig unterwiesen werden.
All patents and applications are to be maintained by payment of fees, taxes and so forth unless you are instructed to the contrary until the due date.

3. Vom Patentamt in Amtsbescheiden angeführte Entgegenhaltungen sind mir nicht zuzusenden, da diese hier beschafft werden.
Any and all citations referred to in Office Actions issued by the Patent Office are not required to be made available to my office, since these will be procured here.

4. Auskünfte, die zur Überwindung der vom Patentamt angeführten Beanstandungen von Nutzen sind, sind mir kostenfrei zu erteilen. Informationen zur Erledigung der Amtsbescheide werden von mir gegeben. Ohne unseren vorherigen Auftrag dürfen Sie keinen Amtsbescheid erledigen.
Any and all particulars being of advantage to overcome objections raised by the Patent Office are to be supplied to my office free of charge. Any and all information for the preparation of responses to Office Actions will be furnished by my office. You must not respond to any Office Action without being briefed by my office in advance.

5. Über alle wichtigen Veränderungen Ihrer Patentgesetze oder Vorschriften bitte ich Sie, mich zu informieren.
You are requested to provide information about all important changes of Patent Laws or Regulations required to be complied with in your country.

6. Alle vom Patentamt eingegangenen Amtsbescheide sind mir zu übersenden.
All Official Letters received from the Patent Office should be communicated to this office.

7. Sie sind nicht befugt, ohne unsere ausdrückliche vorherige Zustimmung bei Neuanmeldungen Überarbeitungen vorzunehmen, z. B. Anpassung der Beschreibung an die landesübliche Praxis. Derartige Überarbeitungen sind mit dem ersten Amtsbescheid zu erledigen.
Without our explicite prior approval given you are not authorized to revise new applications, e.g. adaption of the specification to the national practice. Such revisions are to be made when responding to the first Office Action.

8. In jedem Fall ist die Anmeldung vor Ablauf der angegebenen Priorität einzureichen, auch wenn die Anmeldung noch nicht den Formvorschriften entspricht oder Unterlagen fehlen.
In any case the application is to be filed prior to the expiration of the priority stated, even if the application

PATENTANWALT

DR.-ING. PETER RIEBLING
Dipl.-Ing.

EUROPEAN PATENT & TRADEMARK ATTORNEY

Postfach 3160
D-88113 Lindau (Bodensee)
Telefon (08382) 78025
Telefon (08382) 9692-0
Telefax (08382) 78027
Telefax (08382) 9692-30
E-mail: Riebling@t-online.de

31. August 2001

Europäisches Patentamt
Erhardtstraße 27

80331 München

Amtl. Aktenzeichen : PCT/DE00/00792
Vertretung von : DeTeMobil
Anwaltsakte : 15211.4-D1971-49

Hierdurch wird mitgeteilt, daß der Unterzeichnete die Vertretung zu obiger internationaler Patentanmeldung übernommen hat.

Es wird gebeten, den weiteren Schriftverkehr direkt mit dem Unterzeichneten zu führen.

Die firmenmäßig unterzeichnete Vollmacht und die von den Erfindern zu unterzeichnende Vollmacht werden anliegend überreicht.

Patentanwalt
- Dr. Peter Riebling -

Anlagen

WIG-001/ 4 Vollmachten

PATENTANWALT

DR.-ING. PETER RIEBLING
Dipl.-Ing.

EUROPEAN PATENT & TRADEMARK ATTORNEY

Postfach 3160
D-88113 Lindau (Bodensee)
Telefon (08382) 78025
Telefon (08382) 9692-0
Telefax (08382) 78027
Telefax (08382) 9692-30
E-mail: Riebling@t-online.de

Europäisches Patentamt
Erhardtstraße 27

80331 München

29. August 2001

Amtl. Aktenzeichen : PCT/DE00/00792
Vertretung von : DeTeMobil
Anwaltsakte : 15211.4-D1971-54-ku

Auf den 1. Bescheid vom 21.08.2001 in der internationalen vorläufigen Prüfung

Die Anmelderin überreicht geänderte Patentansprüche 1 bis 17 auf entsprechenden Austauschblättern, sowie überarbeitete Beschreibungsseiten 2, 2a und 3 jeweils in 3-facher Ausfertigung.

Der neue Patentanspruch 1 setzt sich aus den Merkmalen der ursprünglichen Patentansprüche 1,7,8 und 9 zusammen. Der beiliegende Anspruch 4 wurde neu hinzugefügt. Die beiliegenden Ansprüche 2,3 und 5 bis 17 entsprechen den ursprünglichen Ansprüchen 2 bis 6 und 10 bis 19.

In den Ansprüchen wurden ferner redaktionelle Änderungen durchgeführt; so wurde z.B. der Begriff „SIM-Karte" teilweise abgeändert in den Begriff „Teilnehmer-Identitätsmodul" bzw. nur „SIM". Ferner wurden die Patentansprüche durchweg mit Bezugszeichen versehen.

In der Beschreibungseinleitung wurden die Dokumente D1 bis D4 berücksichtigt und der darin offenbarte einschlägige Stand der Technik angegeben.

Die durchgeführten Änderungen gehen auch aus dem beiliegenden Änderungsentwurf hervor, der lediglich zur Kenntnisnahme dient.

Die Prüfungsstelle war der Auffassung, dass der Gegenstand des ursprünglichen Anspruch 1 durch eine Kombination der Dokumente D1, D3 und D4 mit dem Dokument D2 nahegelegt sei. Anspruch 1 wurde nun durch Aufnahme weiterer Merkmale gegenüber dem Stand der Technik abgegrenzt und als einteiliger Anspruch formuliert, da dies im vorliegenden Fall günstiger erscheint als eine zweiteilige Fassung, welche den Anspruch unnötig auseinander reissen würde.

Der Stand der Technik lehrt zwar verschiedene Systeme zur Durchführung einer elektronischen Bezahl-Transaktion bzw. lehrt das Wesen des Bankgeschäfte-Standards HBCI, es ist dem Stand der Technik jedoch nicht zu entnehmen, durch Einrichtung eines HBCI-Gateways eine zur HBCI äquivalente Protokollstruktur auf dem Mobilfunknetz zu schaffen, welche eine Kommunikation einer Mobilstation mit einem HBCI-Bankserver ermöglicht. Dabei sollen die bei HBCI verwendeten Sicherheitsstandards ebenfalls auf die Mobilfunkstrecke angewandt werden.

Diese Lehre ist dem Stand der Technik, auch der Kombination der einzelnen Schriften, nicht zu entnehmen.

Dr.-Ing. P. Riebling
Patentanwalt

Anlagen
Ersatzblätter 2,2a und 3 der Beschreibung
Patentansprüche 1 - 17 auf Ersatzblättern 10 - 12, alle Unterlage jeweils 3-fach
Änderungsentwurf vom 29.08.2001

mobilfunkgestütztem Banking aufzusetzen. Leider ist das für das Internet konzipierte HBCI-Protokoll zu umfangreich für eine direkte Abbildung auf die heutige GSM-Mobilfunkwelt. Dies betrifft sowohl die für die Datenübertragung notwendige Bandbreite, als auch die benötigte Speicherkapazität und Rechenleistung auf Seite des Mobilfunkteilnehmers bzw. dessen Mobilstation.

Den nächstkommenden Stand der Technik definiert die WO-A-97 17678. Es ist ein System zur Durchführung einer elektronischen Bezahltransaktion zwischen zwei oder mehreren Parteien offenbart, die alle über ein hierfür geeignetes Terminal verfügen. Jede Partei verwendet ein elektronisches Zahlungsprotokoll, wobei sich die verwendeten Protokolle der einzelnen Parteien voneinander unterscheiden können. Damit dennoch eine Bezahltransaktion durchgeführt werden kann, ist ein Zahlungs-Gateway eingerichtet, das über verschiedene Interfaces verfügt, welche die einzelnen Zahlungsprotokolle unterstützen und für eine Konvertierung der Protokolldaten von einem Format in ein anderes Format sorgen. Die verwendeten Zahlungsprotokolle basieren nicht auf HBCI- oder HBCI-äquivalenten Übertragungsprotokollen.

Der Aufsatz von Heins, K. et al. „Chipkarten sichern Transaktionen übers Internet", aus der Zeitschrift Elektronik 12/1998, DE, Franzis Verlag GmbH, Seiten 74-79, befasst sich mit der Anwendung und den Vorteilen von chipkartengestützten HBCI (Home Banking Computer Interface)-Nachrichtenübertragungsverfahren. Eine Anwendung dieses Verfahrens zusammen mit mobilfunkgestützten Verfahren ist jedoch nicht erwähnt.

Die WO-A-98 47116 betrifft ein elektronisches Bezahlsystem, bei dem ein Kunde über ein mobiles oder ortsfestes Terminal Bezahltransaktionen durchführen kann. Der Kunde stellt dazu eine Verbindung zu einem Service-Gateway her, das die Bezahltransaktion direkt zwischen dem Kreditinstitut des Kunden und dem Kreditstatut des Händlers steuert und abwickelt. Auch hier werden keine auf HBCI basierenden Übertragungsprotokolle verwendet.

Aus der WO-A-98 26543 ist ein System für die Internet-Telefonie bekannt geworden, wobei ein Gateway vorgesehen ist, das die Verbindung zwischen dem Internet und dem Telefonnetz herstellt.

Es ist Aufgabe der Erfindung, ein Verfahren vorzuschlagen, welches die Nutzung von standardisierten Bankdienstleistungen über Mobilfunk erlaubt, wobei herkömmliche Mobilstationen ohne Zusatzgeräte als kundenseitige HBCI-Plattform eingesetzt werden können.

Diese Aufgabe wird durch die in Anspruch 1 angegebenen Merkmale gelöst.

Grundidee dieser Erfindung ist die Verteilung des kundenseitigen HBCI-Systems auf zwei Komponenten - die in der Mobilstation verwendete SIM-Karte (Teilnehmeridentitätsmodul) und einen HBCI-Gateway.

Es werden dazu zwei Übertragungsstrecken gebildet, erstens zwischen SIM-Karte und HBCI-Gateway und zweitens zwischen HBCI-Gateway und Bankserver. Auf beiden Teilstrecken wird eine kryptographische Sicherung realisiert.

Der HBCI-Gateway wird also in den Übermittlungsweg eingefügt. Dieser entpackt das HBCI-Protokoll und wandelt den Protokollablauf derart, dass eine Verträglichkeit mit der GSM-SIM-Karte und dem GSM-Netzstandard erwirkt wird. Der HBCI-Gateway schliesslich tauscht das gewandelte Protokoll mit einer kundenseitig verwendeten SIM-Karte aus. Es erfolgt demnach eine Transformation zwischen dem bankenseitig verwendeten HBCI und einem auf der Mobilfunkseite verwendeten Übertragungsprotokoll. Die Aufgabe des HBCI-Gateways ist im wesentlichen die Reduktion der zu übertragenden Daten auf ein GSM-kompatibles Maß.

Als Trägerdienst für den Informationsaustausch zwischen HBCI-Gateway und Mobilfunkteilnehmer kann z.B. der Short Message Service oder GPRS dienen.

Aus Sicht des Bankservers wird komplett ein standardkonformes HBCI-Protokoll genutzt, wobei zwischen Bankserver und HBCI-Gateway das durch HBCI definierte Sicherheitsprotokoll Anwendung findet. Zwischen HBCI-Gateway und SIM-Karte wird ein anderes Sicherheitsprotokoll verwendet. Dieses entspricht einem vom Datenumfang her reduzierten, aber sicherheitstechnisch HBCI äquivalenten Protokoll.

Anstelle des beim online-banking üblichen PCs übernimmt nun die SIM-Chipkarte die Funktionen des Kundensystems, sowohl was den Benutzerdialog, als auch was die Sicherheitsfunktionen angeht. Ermöglicht wird dies durch eine neue, standardisierte Technologie mit Namen SAT (SIM Application Toolkit), welcher es der Mobilfunk-Chipkarte (SIM-Karte) erlaubt, die Rolle der Dienstesteuerung wahrzunehmen.

Sowohl die SIM-Karte als auch der Bankrechner kommuniziert jeweils direkt ausschließlich mit dem HBCI- Gateway; dieser nimmt also eine Proxy-Funktion, d.h. eine stellvertretende Funktion des jeweiligen Gegenübers wahr.

Die erwähnte Transformation bringt auch eine Transformation der verwendeten Sicherheitsmechanismen mit sich; während zwischen dem Gateway und der Bankenwelt das HBCI-Protokoll angewendet wird, wird GSM-seitig ein eigenes Sicherheitsprotokoll verwendet.

Gemäß der Erfindung ist vorgesehen, dass ein Verfahren zur Anwendung kommt, das es ermöglicht, kryptographische Schlüssel nach der SIM-Kartenpersonalisierung sicher in der SIM-Karte zu generieren und zu speichern. Hierzu wird vom HBCI-Gateway bzw. der Bank ein spezieller PIN Brief erzeugt. Die Eingabe der PIN am Mobiltelefon generiert den kundenspezifischen Schlüssel in der SIM-Karte.

Patentansprüche

1. Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk, bei dem die Datenübertragung zwischen einem Bankserver (10) einer Bank (9) und einer Mobilstation (1) eines Mobilfunknetzes (6) auf einem HBCI-Übertragungsverfahren aufbaut,
wobei ein HBCI-Gateway (7) in den Übermittlungsweg zwischen dem Bankserver (10) und der Mobilstation (1) geschaltet wird, das eine Transformation zwischen dem bankenseitig verwendeten HBCI-Übertragungsverfahren und einem auf der Mobilfunkseite verwendeten Übertragungsverfahren vornimmt, wobei zwischen dem Bankserver (10) und dem HBCI-Gateway (7) ein durch HBCI definiertes Sicherheitsprotokoll und zwischen dem HBCI-Gateway (7) und einem Teilnehmeridentitätsmodul SIM (3) der Mobilstation (1) ein zweites, kryptographisches Sicherheitsprotokoll verwendet wird, das einem vom Datenumfang her reduzierten aber sicherheitstechnisch dem HBCI Protokoll äquivalenten Protokoll entspricht, wobei ein kryptographischer, teilnehmerspezifischer Schlüssel (Ksms) zur Verwendung im zweiten Sicherheitsprotokoll nach einer regulären Personalisierung der SIM (3) sicher in der SIM (3) generiert und gespeichert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Aufspaltung des mobilfunkseitigen HBCI-Systems in zwei Komponenten, die SIM (3) der Mobilstation (1) und das HBCI-Gateway (7) , erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass zwei Übertragungsstrecken gebildet werden, erstens zwischen SIM (3) und HBCI-Gateway (7) und zweitens zwischen HBCI-Gateway (7) und Bankserver (10).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass als Mobilfunknetz (6) ein GSM-Mobilfunknetz verwendet wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das HBCI-Protokoll vom HBCI-Gateway (7) entpackt und dessen Protokollablauf derart umgewandelt wird, dass eine Verträglichkeit mit der SIM (3) und dem GSM-Mobilfunknetz erwirkt wird, so dass ein Austausch des gewandelten Protokolls mit der SIM (3) möglich ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, dass als Trägerdienst für den Informationsaustausch zwischen HBCI-Gateway (7) und Mobilstation (1) ein GSM Datenübertragungsdienst, insbesondere der Short Message Service, GPRS oder USSD dient.

7. Verfahren nach einem der Ansprüche 1 bis 6, dass auf beiden Teilstrecken eine kryptographische Sicherung realisiert wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, dass die Generierung des teilnehmerspezifischen Schlüssels (Ksms) in der SIM (3) durch Eingabe einer Initialisierungs-PIN an der Mobilstation (1) erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 8, daß die Initialisierungs-PIN zur Generierung des Schlüssels (Ksms) dem Teilnehmer durch die Bank (9) per PIN-Brief mitgeteilt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dass bei der Personalisierung der SIM (3) vom Mobilfunknetzbetreiber zusammen mit der Bankenapplikation ein aus einem Masterschlüssel und einer SIM-kartenindividuellen Zahl abgeleiteter Initialisierungsschlüssel KIV zur Erzeugung der teilnehmerspezifischen Ksms auf die SIM (3) aufgebracht wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dass der Teilnehmer vor einer Subskription des Dienstes die Daten seiner Bank (9) inklusive einer Initialisierungs-PIN erhält.

12. Verfahren nach einem der Ansprüche 1 bis 11, dass bei der Initialisierung der Applikation, d.h. bei Subskription, aus der Initialisierungs-PIN mit Hilfe des KIV der Schlüssel Ksms unter Verwendung der lokalen PIN, der Bankleitzahl und der Kontonummer des Teilnehmers per Triple-DES Verschlüsselung (11) erzeugt wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, dass zur Erzeugung des Ksms im HBCI-Gateway (7) die Initialisierungs-PIN zum Gateway-Betreiber weitergereicht wird.

14. Verfahren nach einem der Ansprüche 1 bis 13, dass die Erzeugung der Initialisierungs-PIN am HBCI-Gateway (7) erfolgt und dieser an die Bank weitergeleitet wird.

15. Verfahren nach einem der Ansprüche 1 bis 14, dass die Authentifikation der beiden beteiligten Stellen, Mobilfunkteilnehmer und HBCI-Gateway (7), durch Wissen über die schriftlich ausgetauschte Initialisierungs-PIN erfolgt.

16. Verfahren nach einem der Ansprüche 1 bis 15, dass zwischen Mobilfunknetzbetreiber und HBCI-Gateway-Betreiber ein Masterkey ausgetauscht wird.

17. Verfahren nach einem der Ansprüche 1 bis 16, dass eine zusätzliche Authentifikation des Teilnehmers über die Kennung seines Mobilanschlusses erfolgt, indem eine Auswertung der Calling-Line-Identification (CLI) erfolgt.

mobilfunkgestütztem Banking aufzusetzen. Leider ist das für das Internet konzipierte HBCI-Protokoll zu umfangreich für eine direkte Abbildung auf die heutige GSM-Mobilfunkwelt. Dies betrifft sowohl die für die Datenübertragung notwendige Bandbreite, als auch die benötigte Speicherkapazität und Rechenleistung auf Seite des Mobilfunkteilnehmers bzw. dessen Mobilstation.

Den nächstkommenden Stand der Technik definiert die WO-A-97 17678. Es ist ein System zur Durchführung einer elektronischen Bezahltransaktion zwischen zwei oder mehreren Parteien offenbart, die alle über ein hierfür geeignetes Terminal verfügen. Jede Partei verwendet ein elektronisches Zahlungsprotokoll, wobei sich die verwendeten Protokolle der einzelnen Parteien voneinander unterscheiden können. Damit dennoch eine Bezahltransaktion durchgeführt werden kann, ist ein Zahlungs-Gateway eingerichtet, das über verschiedene Interfaces verfügt, welche die einzelnen Zahlungsprotokolle unterstützen und für eine Konvertierung der Protokolldaten von einem Format in ein anderes Format sorgen.

Der Aufsatz von Heins, K. et al. „Chipkarten sichern Transaktionen übers Internet", aus der Zeitschrift Elektronik 12/1998, DE, Franzis Verlag GmbH, Seiten 74-79, befasst sich mit der Anwendung und den Vorteilen von chipkartengestützten HBCI (Home Banking Computer Interface)-Nachrichtenübertragungsverfahren. Eine Anwendung dieses Verfahrens zusammen mit mobilfunkgestützten Verfahren ist jedoch nicht erwähnt.

Die WO-A-98 47116 betrifft ein elektronisches Bezahlsystem, bei dem ein Kunde über ein mobiles oder ortsfestes Terminal Bezahltransaktionen durchführen kann. Der Kunde stellt dazu eine Verbindung zu einem Service-Gateway her, das die Bezahltransaktion direkt zwischen dem Kreditinstitut des Kunden und dem Kreditstatut des Händlers steuert und abwickelt.

Aus der WO-A-98 26543 ist ein System für die Internet-Telefonie bekannt geworden, wobei ein Gateway vorgesehen ist, das die Verbindung zwischen dem Internet und dem Telefonnetz herstellt.

Aus Sicht des Bankservers wird komplett ein standardkonformes HBCI-Protokoll genutzt, wobei zwischen Bankserver und HBCI-Gateway das durch HBCI definierte Sicherheitsprotokoll Anwendung findet. Zwischen HBCI-Gateway und SIM-Karte wird ein anderes Sicherheitsprotokoll verwendet. Dieses entspricht einem vom Datenumfang her reduzierten, aber sicherheitstechnisch HBCI äquivalenten Protokoll.

Anstelle des beim online-banking üblichen PCs übernimmt nun die SIM-Chipkarte die Funktionen des Kundensystems, sowohl was den Benutzerdialog, als auch was die Sicherheitsfunktionen angeht. Ermöglicht wird dies durch eine neue, standardisierte Technologie mit Namen SAT (SIM Application Toolkit), welcher es der Mobilfunk-Chipkarte (SIM-Karte) erlaubt, die Rolle der Dienstesteuerung wahrzunehmen.

Sowohl die SIM-Karte als auch der Bankrechner kommuniziert jeweils direkt ausschließlich mit dem HBCI- Gateway; dieser nimmt also eine Proxy-Funktion, d.h. eine stellvertretende Funktion des jeweiligen Gegenübers wahr.

Die erwähnte Transformation bringt auch eine Transformation der verwendeten Sicherheitsmechanismen mit sich; während zwischen dem Gateway und der Bankenwelt das HBCI-Protokoll angewendet wird, wird GSM-seitig ein eigenes Sicherheitsprotokoll verwendet.

Gemäß ~~In einer bevorzugten Weiterbildung~~ der Erfindung ist vorgesehen, dass ein Verfahren zur Anwendung kommt, das es ermöglicht, kryptographische Schlüssel nach der SIM-Kartenpersonalisierung sicher in der SIM-Karte zu generieren und zu speichern. Hierzu wird vom HBCI-Gateway bzw. der Bank ein spezieller PIN Brief erzeugt. Die Eingabe der PIN am Mobiltelefon generiert den kundenspezifischen Schlüssel in der SIM-Karte

Patentansprüche

1. Verfahren zur Nutzung von standardisierten Bankdienstleistungen über Mobilfunk, bei dem~~wobei~~ die Datenübertragung zwischen einem Bankserver (10) einer Bank (9) und einer Mobilstation (1) eines Mobilfunknetzes (6) auf einem~~dem~~ HBCI-Übertragungsverfahren aufbaut,
~~dadurch gekennzeichnet,~~ wobei
~~dass~~ ein HBCI-Gateway (7) in den Übermittlungsweg zwischen dem Bankserver (10) und der Mobilstation (1) geschaltet wird, der eine Transformation zwischen dem bankenseitig verwendeten HBCI-Übertragungsverfahren und einem auf der Mobilfunkseite verwendeten Übertragungsverfahren vornimmt, wobei zwischen dem Bankserver (10) und dem HBCI-Gateway (7) ein durch HBCI definiertes Sicherheitsprotokoll und zwischen dem HBCI-Gateway (7) und einem Teilnehmeridentitätsmodul SIM (3) der Mobilstation (1) ein zweites kryptographisches Sicherheitsprotokoll verwendet wird, das einem vom Datenumfang her reduzierten aber sicherheitstechnisch dem HBCI Protokoll äquivalenten Protokoll entspricht, wobei ein kryptographischer, teilnehmerspezifischer Schlüssel (Ksms) zur Verwendung im zweiten Sicherheitsprotokoll nach einer regulären Personalisierung der SIM (3) sicher in der SIM (3) generiert und gespeichert wird.

~~2.~~

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Aufspaltung des mobilfunkseitigen ~~kundenseitigen~~ HBCI-Systems in zwei Komponenten, die SIM (3) ~~-Karte~~ der Mobilstation (1) und da~~se~~n HBCI-Gateway (7), erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass zwei Übertragungsstrecken gebildet werden, erstens zwischen SIM (3) ~~-Karte~~ und HBCI-Gateway (7) und zweitens zwischen HBCI-Gateway (7) und Bankserver (10).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass als Mobilfunknetz (6) ein GSM-Mobilfunknetz verwendet wird,

5. Verfahren nach einem der Ansprüche 1 bis 4~~3~~, dadurch gekennzeichnet, dass das HBCI-Protokoll vom HBCI-Gateway (7) entpackt und dessen Protokollablauf derart umgewandelt wird, dass eine Verträglichkeit mit der ~~GSM-~~SIM (3)~~-Karte~~ und dem GSM-MobilfunkNnetz (6) erwirkt wird, so dass ein Austausch des gewandelten Protokolls mit der SIM (3)~~-Karte~~ möglich ist.

6. Verfahren nach einem der Ansprüche 1 bis 5~~4~~, dass als Trägerdienst für den Informationsaustausch zwischen HBCI-Gateway (7) und Mobilstation (1) ein GSM Datenübertragungsdienst, insbesondere der Short Message Service, GPRS oder USSD dient.

7. Verfahren nach einem der Ansprüche 1 bis 6~~5~~, dass auf beiden Teilstrecken eine kryptographische Sicherung realisiert wird.

~~8. Verfahren nach einem der Ansprüche 1 bis 6, dass zwischen Bankserver und HBCI-Gateway das durch HBCI definierte Sicherheitsprotokoll-Anwendung findet und zwischen HBCI-Gateway und SIM-Karte ein zweites Sicherheitsprotokoll verwendet wird.~~

~~8. Verfahren nach einem der Ansprüche 1 bis 7, dass das zweite Sicherheitsprotokoll einem vom Datenumfang her reduzierten aber sicherheitstechnisch HBCI-äquivalenten Protokoll entspricht.~~

~~8. Verfahren nach einem der Ansprüche 1 bis 8, dass ein kryptographischer, teilnehmerspezifischer Schlüssel (Ksms) zur Verwendung im zweiten Sicherheitsprotokoll nach der regulären SIM-Kartenpersonalisierung sicher in der SIM-Karte generiert und gespeichert wird.~~

8. Verfahren nach einem der Ansprüche 1 bis 7~~9~~, dass die Generierung des teilnehmerspezifischen Schlüssels (Ksms) in der SIM (3) ~~Karte~~ durch Eingabe einer Initialisierungs-PIN an der~~m~~ Mobilstation (1)~~telefon~~ erfolgt~~generiert wird~~.

9. Verfahren nach einem der Ansprüche 1 bis 8~~10~~, daß die Initialisierungs-PIN zur Generierung des Schlüssels (Ksms) dem Teilnehmer durch die Bank (9) per PIN-Brief mitgeteilt wird.

10. Verfahren nach einem der Ansprüche 1 bis 9~~11~~, dass bei der ~~Kartenp~~Personalisierung der SIM vom Mobilfunknetzbetreiber zusammen mit der Bankenapplikation ein aus einem Masterschlüssel und einer SIM-~~K~~kartenindividuellen Zahl abgeleiteter Initialisierungsschlüssel KIV~~,~~ zur Erzeugung der teilnehmerspezifischen Ksms auf die~~alle~~ SIM (3) ~~Karten~~ aufgebracht wird.

11. Verfahren nach einem der Ansprüche 1 bis 10~~12~~, dass der Teilnehmer vor einer Subskription des Dienstes die Daten seiner Bank (9) inklusive einer Initialisierungs-PIN erhält.

12. Verfahren nach einem der Ansprüche 1 bis 11~~13~~, dass bei der Initialisierung der Applikation, d.h. bei Subskription~~Subscription,~~ aus der Initialisierungs-PIN mit Hilfe des KIV der Schlüssel Ksms unter Verwendung der lokalen PIN, der Bankleitzahl und der Kontonummer des Teilnehmers per Triple-DES Verschlüsselung (11) erzeugt wird.

13. Verfahren nach einem der Ansprüche 1 bis 12~~14~~, dass zur Erzeugung des Ksms im HBCI-Gateway (7) die Initialisierungs-PIN zum Gateway-Betreiber weitergereicht wird.

14. Verfahren nach einem der Ansprüche 1 bis 13~~14~~, dass die Erzeugung der Initialisierungs-PIN am HBCI-Gateway (7) erfolgt und dieser an die Bank (9) weitergeleitet wird.

15. Verfahren nach einem der Ansprüche 1 bis 14~~16~~, dass die Authentifikation der beiden beteiligten Stellen, Mobilfunkteilnehmer und HBCI-Gateway (7), durch Wissen über die schriftlich ausgetauschte Initialisierungs-PIN erfolgt.

16. Verfahren nach einem der Ansprüche 1 bis 15~~17~~, dass zwischen Mobilfunknetzbetreiber und HBCI-Gateway-Betreiber ein Masterkey ausgetauscht wird.

17. Verfahren nach einem der Ansprüche 1 bis 16~~18~~, dass eine zusätzliche Authentifikation des Teilnehmers über die Kennung seines Mobilanschlusses erfolgt~~en~~, indem eine Auswertung der Calling-Line-Identification (CLI) erfolgt.

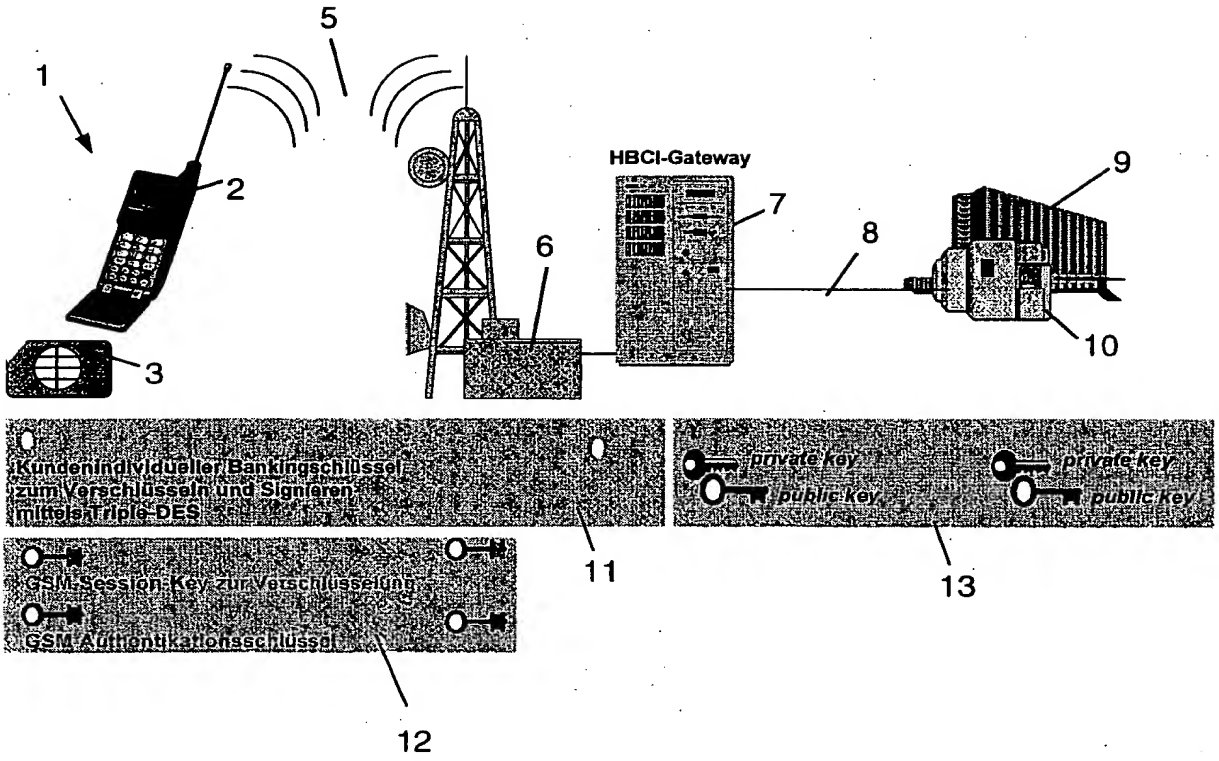
1
2
3
5
6
HBCI-Gateway
7
8
9
10
Kundenindividueller Bankingschlüssel zum Verschlüsseln und Signieren mittels Triple-DES
11
private key
public key
private key
public key
13
GSM-Session-Key zur Verschlüsselung
GSM-Authentikationsschlüssel
12

FIG. 1

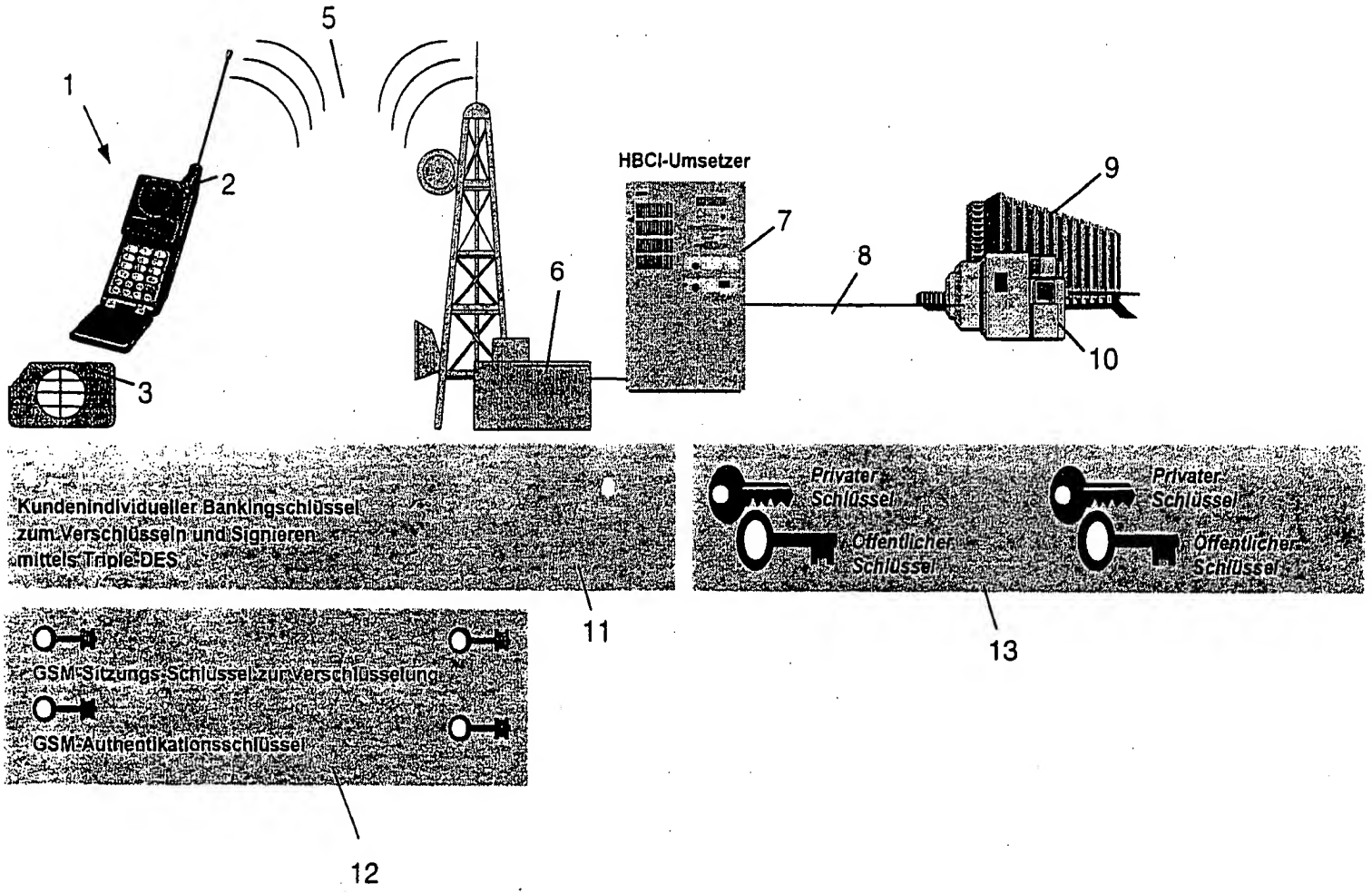
1
2
3
5
6
HBCI-Umsetzer
7
8
9
10
Kundenindividueller Bankingschlüssel
zum Verschlüsseln und Signieren
mittels Triple-DES
11
Privater Schlüssel
Öffentlicher Schlüssel
Privater Schlüssel
Öffentlicher Schlüssel
13
GSM-Sitzungs-Schlüssel zur Verschlüsselung
GSM-Authentikationsschlüssel
12

FIG. 1

Online-Subscription

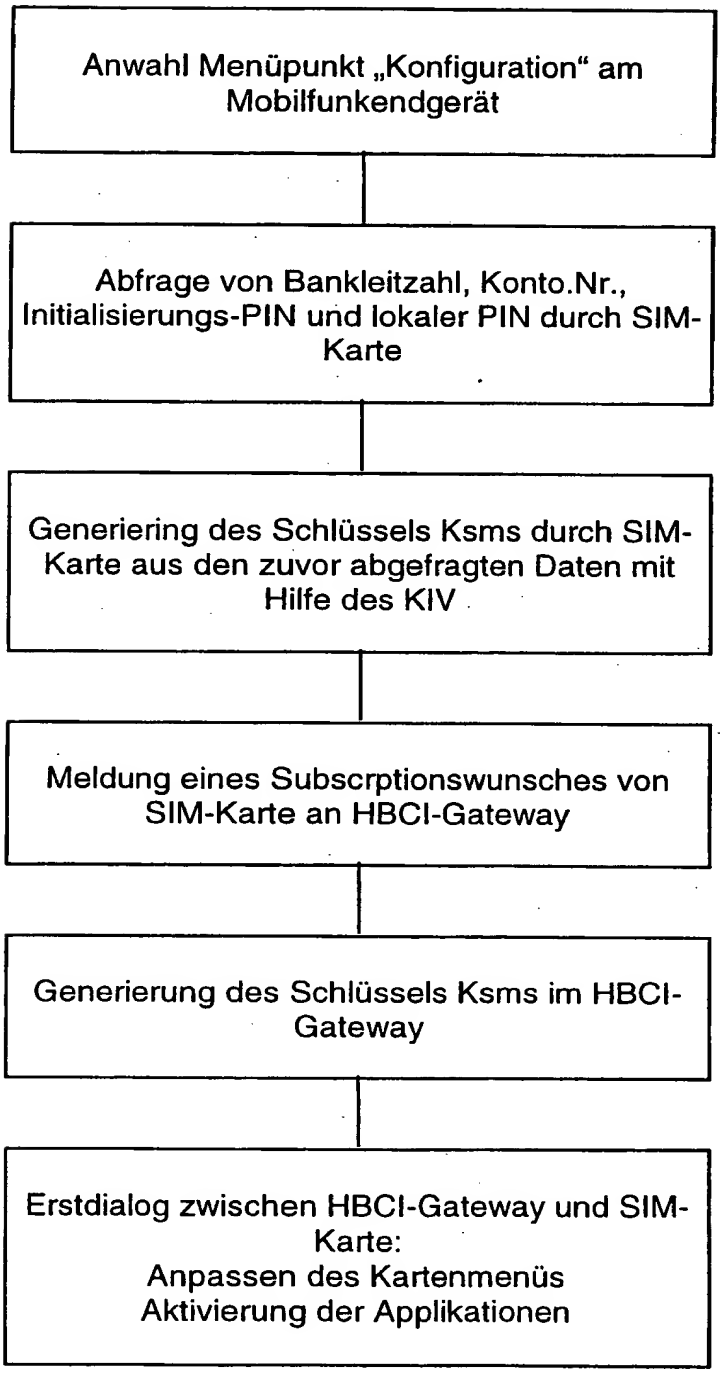

FIG. 2